UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/789,311	02/27/2004	Sheueling Chang Shantz	6000-31500	9201

7590 06/19/2007

Robert C. Kowert
Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
06/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/789,311	Applicant(s) SHANTZ ET AL.	
	Examiner Carlton V. Johnson	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 27 February 2004.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-67 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-67 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 27 February 2004 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 7-26-2004/12-10-2004.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed on **2-27-2004**.

2. Claims **1 - 67** are pending. Claims **1, 21, 38, 53, 66** are independent.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims **1 - 67** are rejected under 35 U.S.C. 101 because the claimed invention is based on non-statutory subject matter and directed towards nothing more than the abstract idea of a mathematical algorithm. Abstract ideas are not eligible for patent protection. A claimed invention reciting a computer program product that solely calculates a mathematical formula or a computer readable medium that solely stores a mathematical formula is not directed to the type of subject matter eligible for patent protection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim **1 - 67** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Gressel et al.** (US Patent No. **6,748,410**) in view of **Stribaek et al.** (US Patent No. **6,181,484**).

Each independent section of the claimed invention will be addressed. The independent claim and the dependent claims based upon that independent claim recite instructions utilized to perform mathematical procedures or steps, such as multiplication and addition (i.e. summing), for an algorithm utilizing computer system processor(s) and system register(s).

Regarding Claims 1 - 20, Gressel discloses a method comprising: feeding back high order bits of a previously executed arithmetic instruction, generated by a first plurality of arithmetic structures, to a second plurality of arithmetic structures; and using the second arithmetic structures, generating a first partial result of a currently executed arithmetic instruction, the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number, the summing of the high order bits being performed during multiplication of the first number and the second number, the summing and at least a portion of the multiplication being performed in the second arithmetic structures.

(see Gressel:

col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines

40-49: arithmetic operation or instructions; col. 31, lines 44-46; col. 41, lines 3-5: arithmetic structure; col. 2, lines 31-37: multiplication two values, summing two values utilizing partial (i.e. bit operations, any bit length, high order bits, low order bits) results from previous multiplication; col. 6, lines 20-25: adder; col. 31, lines 46-48; col. 6, line 66 - col. 7, line 9; col. 31, lines 44-46: carry-save adder; col. 49, lines 47-51: carry-out; col. 2, lines 4-9; col. 5, lines 58-67; col. 41, lines 20-23: register usage; col. 8, lines 59-60; col. 53, lines 13-19: XOR operations; col. 29, lines 43-49: redundant representation of numbers; col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation)

Gressel discloses the capability for the multiplication of parameters and circuit, array operations. Gressel does not specifically disclose the usage of Wallace tree multiplication, and extended carry operations. However, Stribaek discloses the usage of Wallace tree columns and multiplications of parameters, and the usage of extended carry operations.

(see Stribaek:

col. 9, lines 10-24; col. 9, lines 37-39: Wallace tree; col. 5, lines 41-45: extended carry operations; col. 7, lines 31-37; col. 9, lines 10-14: carry-save adder; col. 2, line 66 - col. 3, line 6: public key cryptographic calculations)

It would have been obvious to one of ordinary skill in the art to modify Gressel as taught by Stribaek to enable the capability for the usage of Wallace tree multiplication. One of ordinary skill in the art would have been motivated to employ the teachings of Stribaek in order to enable the capability for extended precision in arithmetic calculations due to extensive and increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67: " *... Public-key cryptosystems have been used extensively for user authentication and secure key exchange, while private-key cryptography has been used extensively to encrypt communication channels. As the use of public-key cryptosystems increases, it becomes desirable to increase the performance of extended-precision modular arithmetic calculations. ...* ")

Regarding Claims 21 - 37, Gressel discloses a method comprising: feeding back high order bits of a previously executed arithmetic instruction, from a first plurality of arithmetic structures generating the high order bits, to a second plurality of arithmetic structures; supplying a third number to the second plurality of arithmetic structures; and using the second arithmetic structures generating a first partial result of a currently executed arithmetic instruction, the first partial result being a representation of the high order bits summed with, low order bits of a result of a first number multiplied by a second number, and summed with the third number, the summing of the high order bits and the summing of the third number being performed during multiplication of the first number and the second number, the summing and a portion of the multiplication being performed in the second arithmetic structures.

(see Gressel:

col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions; col. 31, lines 44-46; col. 41, lines 3-5: arithmetic structure; col. 2, lines 31-37: multiplication two values, summing two values utilizing partial (i.e. bit operations, any bit length, high order bits, low order bits) results from previous multiplication; col. 6, lines 20-25: adder; col. 31, lines 46-48; col. 6, line 66 - col. 7, line 9; col. 31, lines 44-46: carry-save adder; col. 49, lines 47-51: carry-out; col. 2, lines 4-9; col. 5, lines 58-67; col. 41, lines 20-23: register usage; col. 8, lines 59-60; col. 53, lines 13-19: XOR operations; col. 29, lines 43-49: redundant representation of numbers; col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation)

Gressel discloses the capability for the multiplication of parameters and circuit, array operations. Gressel does not specifically disclose the usage of Wallace tree multiplication, and extended carry operations. However, Stribaek discloses the usage of Wallace tree columns and multiplications of parameters, and the usage of extended carry operations.

(see Stribaek:

col. 9, lines 10-24; col. 9, lines 37-39: Wallace tree; col. 5, lines 41-45: extended carry operations; col. 7, lines 31-37; col. 9, lines 10-14: carry-save adder; col. 2, line 66 - col. 3, line 6: public key cryptographic calculations)

It would have been obvious to one of ordinary skill in the art to modify Gressel as taught by Stribaek to enable the capability for the usage of Wallace tree multiplication. One of ordinary skill in the art would have been motivated to employ the teachings of Stribaek in order to enable the capability for extended precision in arithmetic calculations due to extensive and increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67)

Regarding Claims 38 - 52, Gressel discloses an apparatus comprising: a first plurality of arithmetic structures generating high order bits for an arithmetic operation that includes a multiplication operation; a second plurality of arithmetic structures generating low order bits of the arithmetic operation; and wherein the second arithmetic structures are coupled to receive the high order bits generated by the first plurality of arithmetic structures during a previous arithmetic operation and to generate a first partial result of the arithmetic operation, the first partial result representing the high order bits summed with low order bits of a multiplication result of the multiplication operation.

(see Gressel:

col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions; col. 31, lines 44-46; col. 41, lines 3-5:

arithmetic structure; col. 2, lines 31-37: multiplication two values, summing two values utilizing partial (i.e. bit operations, any bit length, high order bits, low order bits) results from previous multiplication; col. 6, lines 20-25: adder; col. 31, lines 46-48; col. 6, line 66 - col. 7, line 9; col. 31, lines 44-46: carry-save adder; col. 49, lines 47-51: carry-out; col. 2, lines 4-9; col. 5, lines 58-67; col. 41, lines 20-23: register usage; col. 8, lines 59-60; col. 53, lines 13-19: XOR operations; col. 29, lines 43-49: redundant representation of numbers; col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation)

Gressel discloses the capability for the multiplication of parameters and circuit, array operations. Gressel does not specifically disclose the usage of Wallace tree multiplication, and extended carry operations. However, Stribaek discloses the usage of Wallace tree columns and multiplications of parameters, and the usage of extended carry operations.

(see Stribaek:

col. 9, lines 10-24; col. 9, lines 37-39: Wallace tree; col. 5, lines 41-45: extended carry operations; col. 7, lines 31-37; col. 9, lines 10-14: carry-save adder; col. 2, line 66 - col. 3, line 6: public key cryptographic calculations)

It would have been obvious to one of ordinary skill in the art to modify Gressel as taught by Stribaek to enable the capability for the usage of Wallace tree multiplication.

One of ordinary skill in the art would have been motivated to employ the teachings of Stribaek in order to enable the capability for extended precision in arithmetic calculations due to extensive and increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67)

Regarding Claims 53 - 65, Gressel discloses an apparatus comprising: a first plurality of arithmetic structures generating high order bits for an arithmetic operation that includes a multiplication operation of a first and a second number; a second plurality of arithmetic structures generating low order bits of the arithmetic operation; and wherein the second arithmetic structures are coupled to receive the high order bits generated by the first plurality of arithmetic structures during a previous arithmetic operation and are coupled to receive a third number and are coupled to generate a first partial result of the arithmetic operation, the first partial result representing the high order bits summed with, low order bits of a multiplication result of the multiplication operation, and summed with the third number.

(see Gressel:

> col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions; col. 31, lines 44-46; col. 41, lines 3-5: arithmetic structure; col. 2, lines 31-37: multiplication two values, summing two values utilizing partial (i.e. bit operations, any bit length, high order bits, low order bits) results from previous multiplication; col. 6, lines 20-25: adder; col. 31, lines

46-48; col. 6, line 66 - col. 7, line 9; col. 31, lines 44-46: carry-save adder; col. 49, lines 47-51: carry-out; col. 2, lines 4-9; col. 5, lines 58-67; col. 41, lines 20-23: register usage; col. 8, lines 59-60; col. 53, lines 13-19: XOR operations; col. 29, lines 43-49: redundant representation of numbers; col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation)

Gressel discloses the capability for the multiplication of parameters and circuit, array operations. Gressel does not specifically disclose the usage of Wallace tree multiplication, and extended carry operations. However, Stribaek discloses the usage of Wallace tree columns and multiplications of parameters, and the usage of extended carry operations.

(see Stribaek:

col. 9, lines 10-24; col. 9, lines 37-39: Wallace tree; col. 5, lines 41-45: extended carry operations; col. 7, lines 31-37; col. 9, lines 10-14: carry-save adder; col. 2, line 66 - col. 3, line 6: public key cryptographic calculations)

It would have been obvious to one of ordinary skill in the art to modify Gressel as taught by Stribaek to enable the capability for the usage of Wallace tree multiplication. One of ordinary skill in the art would have been motivated to employ the teachings of Stribaek in order to enable the capability for extended precision in arithmetic calculations due to extensive and increasing usage of public key cryptography. (see

Stribaek col. 1, lines 61-67)

Regarding Claim 66, Gressel discloses an apparatus comprising: means for feeding back high order bits of a previously executed arithmetic instruction, generated by a first plurality of arithmetic structures, to a second plurality of arithmetic structures generating low order bits of a currently executed arithmetic instruction; and means for using the second arithmetic structures to generate a first partial result of the currently executed arithmetic instruction, the first partial result representing the high order bits of the previously executed arithmetic instruction that are summed with low order bits of a multiplication result of a first number multiplied by a second number.

(see Gressel:

col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions; col. 31, lines 44-46; col. 41, lines 3-5: arithmetic structure; col. 2, lines 31-37: multiplication two values, summing two values utilizing partial (i.e. bit operations, any bit length, high order bits, low order bits) results from previous multiplication; col. 6, lines 20-25: adder; col. 31, lines 46-48; col. 6, line 66 - col. 7, line 9; col. 31, lines 44-46: carry-save adder; col. 49, lines 47-51: carry-out; col. 2, lines 4-9; col. 5, lines 58-67; col. 41, lines 20-23: register usage; col. 8, lines 59-60; col. 53, lines 13-19: XOR operations; col. 29, lines 43-49: redundant representation of numbers; col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32:

arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation)

Gressel discloses the capability for the multiplication of parameters and circuit, array operations. Gressel does not specifically disclose the usage of Wallace tree multiplication, and extended carry operations. However, Stribaek discloses the usage of Wallace tree columns and multiplications of parameters, and the usage of extended carry operations.

(see Stribaek:

col. 9, lines 10-24; col. 9, lines 37-39: Wallace tree; col. 5, lines 41-45: extended carry operations; col. 7, lines 31-37; col. 9, lines 10-14: carry-save adder; col. 2, line 66 - col. 3, line 6: public key cryptographic calculations)

It would have been obvious to one of ordinary skill in the art to modify Gressel as taught by Stribaek to enable the capability for the usage of Wallace tree multiplication. One of ordinary skill in the art would have been motivated to employ the teachings of Stribaek in order to enable the capability for extended precision in arithmetic calculations due to extensive and increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67)

Regarding Claim 67, Gressel discloses an apparatus comprising: means for feeding back high order bits of a previously executed arithmetic instruction, from a first plurality of arithmetic structures generating the high order bits, to a second plurality of arithmetic structures generating low order bits of a currently executed arithmetic instruction; means for supplying a third number to the second plurality of arithmetic structures; and means for using the second arithmetic structures to generate a first partial result, the first partial result being a representation of the high order bits of the previously executed arithmetic instruction summed with low order bits of a result of a first number multiplied by a second number, and summed with the third number.

(see Gressel:

col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions; col. 31, lines 44-46; col. 41, lines 3-5: arithmetic structure; col. 2, lines 31-37: multiplication two values, summing two values utilizing partial (i.e. bit operations, any bit length, high order bits, low order bits) results from previous multiplication; col. 6, lines 20-25: adder; col. 31, lines 46-48; col. 6, line 66 - col. 7, line 9; col. 31, lines 44-46: carry-save adder; col. 49, lines 47-51: carry-out; col. 2, lines 4-9; col. 5, lines 58-67; col. 41, lines 20-23: register usage; col. 8, lines 59-60; col. 53, lines 13-19: XOR operations; col. 29, lines 43-49: redundant representation of numbers; col. 1, lines 39-45; col. 5, lines 23-25: acceleration, improvements of arithmetic operations; col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines 18-22: processor utilization for key generation)

Gressel discloses the capability for the multiplication of parameters and circuit, array operations. Gressel does not specifically disclose the usage of Wallace tree multiplication, and extended carry operations. However, Stribaek discloses the usage of Wallace tree columns and multiplications of parameters, and the usage of extended carry operations.

(see Stribaek:

col. 9, lines 10-24; col. 9, lines 37-39: Wallace tree; col. 5, lines 41-45: extended carry operations; col. 7, lines 31-37; col. 9, lines 10-14: carry-save adder; col. 2, line 66 - col. 3, line 6: public key cryptographic calculations)

It would have been obvious to one of ordinary skill in the art to modify Gressel as taught by Stribaek to enable the capability for the usage of Wallace tree multiplication. One of ordinary skill in the art would have been motivated to employ the teachings of Stribaek in order to enable the capability for extended precision in arithmetic calculations due to extensive and increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

6, 11, 07

C.J.
CVJ
May 28, 2007